REMARKS

Claims 1-28 and 33-34 are pending in the present application. Claims 1, 4, 7, 10, 13, 17, 21 and 25 are independent claims.

35 U.S.C. §101 Rejection

Claims 7-9 and 21-24 are rejected as being drawn to non-statutory subject matter. Applicant traverses this rejection.

Claims 7-9 and 21-24 are each drawn to structural limitations, i.e., apparatuses. The Examiner's position is that the "means for" language reads only upon computer program modules, which are not structural (See Page 2 of the 6/25/2008 Office Action). Applicant respectfully disagrees.

For example, claim 7 recites a "means for transmitting". The claimed "means for transmitting" reads on a transmitter (e.g., see [0013], [0031], [0034], [0035], etc.). In an example, as noted on [0035], the transmitter can be included within the communication device (CD) 12, which may correspond to the "first communication device" as recited in claim 7. Likewise, each "means for encrypting" and "means for encapsulating" may also read upon the CD 12 (or CD 108 of FIG. 3), which may correspond to the "first communication device" as recited in claim 7. Thus, while computer program modules may be involved in the functionality recited in claim 7, the actual means that performs the functionality is structural, as evidenced at least by CD 12 and CD 108.

With respect to Figure 3, the "first communication device" of claim 7, and thereby the "means for encapsulating", "means for encrypting" and "means for transmitting" limitations, may read upon the CD 108 in Figure 3 (e.g., corresponding to the speaker, which is encrypting and sending media packets for a PTT call), and the "means" (i.e., the means for receiving and means

for determining) limitations in claim 21 may read upon CDs 112 and/or 116, which correspond to a listener in the PTT call (e.g., which receives and decodes the media packets). Clearly, in either claim 7 and 21, more than mere computer program modules are involved because computer programs, in a vacuum, cannot transmit or receive information, and claim 7 recites the "means for transmitting" whereas claim 21 recites the "means for receiving".

Accordingly, Applicant respectfully submits that claims 7-9 and 21-24 read on statutory subject matter, and requests that this rejection be withdrawn.

35 U.S.C. 103(a) Alden in view of Citta

Claims 1, 4, 7, 13-28, 33 and 34 are rejected under 35 U.S.C. § 103(a) as being unpatentable over Alden (6,101,543) in view of Citta (4,771,458) and in further view of Barnett (6,661,896). Applicant respectfully traverses this art grounds of rejection.

In Applicant's previous Response of 4/11/2008, Applicant discussed Alden and Citta in detail, and discussed that each of Alden and Citta was silent regarding "encrypting a first data frame based on a first unique code ... said first unique code being *derived from a first sequential code*" and "encapsulating said first encrypted data frame in a first transport frame, *said first transport frame comprising a first portion and a second portion of said first sequential code*" (Emphasis added) as recited in independent claim 1 and similarly recited in independent claims 4, 7, 10, 13, 17, 21 and 25. The Examiner appears receptive to this argument, as the Examiner has stated that "neither of [Alden or Citta] explicitly discloses a step of deriving a unique encryption code based on sequential code" (See Pages 7-8 of the 6/25/2008 Office Action). However, the Examiner now cites to Barnett as disclosing this particular deficiency of Alden and Citta.

Discussion of Alden and Citta

As an initial matter, Applicant will briefly address Alden and Citta and their respective failure to disclose or suggest the claim language emphasized in the preceding paragraph.

The Examiner has already acknowledged that Alden fails to "disclose that the encryption is based on sequential code encryption" (See Page 7 of the 6/25/2008 Office Action). Further, as discussed in more detail in Applicant's previous response of 4/11/2008, Citta discloses applying different encryption to different data packets (i.e., global packets vs. individual subscriber packets). However, both Alden and Citta fail to disclose or suggest deriving a unique encryption code based on a sequential code, using the unique encryption code to encrypt a data frame and then encapsulating the sequential code within the data frame. The only components of the data frame in Citta are 48 data bits (i.e., content) and the 16 CRC bits used to determine whether authorization is sufficient (e.g., "each packet consists of 48 bits of 'data' and 16 bits of CRC code" at Column 3, lines 49-51 of Citta). Likewise, no code used to establish the encryption key in Alden is added to the data frame by the pseudo network adapter 259. The Examiner alleges that Alden discloses this limitation at Column 3, lines 19-21, but Alden merely discloses a general encapsulation of tunnel data frames in this section, and is silent regarding what is comprised within the tunnel data frames here.

Discussion of Barnett

Barnett is directed to a computer network security system and method. Barnett teaches applying a key generation algorithm to a predetermined character string at a workstation to generate a unique encryption key and a transport key (e.g., See Barnett at Col. 3, lines 44-55). A data packet is encrypted based on the unique encryption key (e.g., See Barnett at Col. 3, lines 56-57). The encrypted data packet, along with the transport key, is sent to a server (e.g., See Barnett

at Col. 3, lines 58-59). The server extracts the transport key, compares the transport key with a predefined list of transport keys maintained at the server, loads the unique encryption key corresponding to a matching transport key from the list and decrypts the packet based on the unique encryption key (e.g., See Barnett at Col. 3, lines 59-67, also see "*If the transport key is not in the predefined list of transport keys, the packet is discarded. If the transport key is in the list, the packet is decrypted using the encryption key within the table*" at Col. 5, lines 2-6 of Barnett). The server will then use the same transport and encryption keys for packets that are sent back to the workstation from the server (See Col. 5, lines 18-30 of Barnett).

Accordingly, the character string is used at the workstation to derive both the unique encryption key and the transport key, and only the transport key is included in the packet along with the encrypted data. The character string is used by remote workstations to generate encryption and transport keys for use in communication with the server, but the character strings is not actually transmitted to the server; rather, the transport key is included in the actual packet, while the packet data is encrypted based on the encryption key.

Deficiencies of Barnett

The Examiner reads the claimed "sequential code" upon Barnett's character string (See Page 8 of the 6/25/2008 Office Action). However, as noted above, Barnett's character string is not included in the data packet transmission. Rather, only the encrypted data and the transport key are included in the data packet. Accordingly, even if one were to accept the Examiner's interpretation that the claim limitation "said first unique code being derived from a first sequential code" reads on Barnett such that the "first unique code" corresponds to the unique encryption key, and the "first sequential code" corresponds to the character string, Barnett under this interpretation clearly could not disclose or suggest "encapsulating said first encrypted data

frame in a first transport frame, *said first transport frame comprising a first portion and a second portion of said first sequential code*" (Emphasis added) as recited in independent claim 1 and similarly recited in independent claims 4, 7, 10, 13, 17, 21 and 25 because the character string in Barnett is not included in the transport frame. Also, if the Examiner were to change the above-noted interpretation to read the "sequential code" on the transport key, Applicant notes that the transport key is not used to derive the unique encryption key; rather, the character string is used to derive both keys (e.g., See Barnett at Col. 3, lines 44-56).

Accordingly, neither Alden, Citta nor Barnett teach using a code to derive an encryption key and then including the code in a data packet that is encrypted according to the encryption key. This is admitted with respect to Alden and Citta, and Barnett teaches the inclusion of a separately derived transport key in the packet, and not the character string (e.g., upon which the Examiner reads the claimed "code") that is used to derive the encryption and transport keys.

In view of the above remarks, Applicant respectfully submits that the combination of Alden, Citta and Barnett fail to disclose or suggest "encrypting a first data frame based on a first unique code ... said first unique code being *derived from a first sequential code*" and "encapsulating said first encrypted data frame in a first transport frame, *said first transport frame comprising a first portion and a second portion of said first sequential code*" (Emphasis added) as recited in independent claim 1 and similarly recited in independent claims 4, 7, 10, 13, 17, 21 and 25.

As such, claims 14-16, 18-20, 22-24, 26-28 and 33-34, dependent upon independent claims 1, 13, 17, 21 and 25, respectively, are likewise allowable over Alden in view of Citta and in further view of Barnett at least for the reasons expressed above with respect to independent claims 1, 13, 17, 21 and 25, respectively.

Applicant respectfully requests that the Examiner withdraw this art grounds of rejection.

35 U.S.C. 103(a) Alden in view of Citta, Barnett and Perlman

Claims 2, 5, 8 and 11 stand rejected under 35 USC § 103(a) as being unpatentable over Alden in view of Citta and Barnett and further in view of Perlman (US 6363480). Applicant respectfully traverses this art grounds of rejection.

Initially, Applicant agrees with the Examiner regarding the failure of Alden, Barnett and Citta in disclosing or anticipating certain claim limitations present within claims 2, 5, 8 and 11. The Examiner alleges, however, that Perlman discloses these particular claim limitations.

Perlman is directed to a method of ephemeral decryptability. A review of Perlman indicates that Perlman fails to cure the suggestion and disclosure deficiencies of Alden in view of Citta and Barnett related to independent claims 1, 4, 7 and 10. As such, claims 2, 5, 8 and 11, dependent upon independent claims 1, 4, 7 and 10, are likewise allowable over Alden in view of Citta and Barnett and further in view of Perlman at least for the reasons given above with respect to independent claims 1, 4, 7 and 10.

Applicant respectfully requests that the Examiner withdraw this art grounds of rejection.

35 U.S.C. 103(a) Alden in view of Citta and Barnett and further in view of Semper

Claims 3, 6, 9 and 12 stand rejected under 35 USC § 103(a) as being unpatentable over Aldre in view of Citta and Barnett and further in view of Semper (6,657,984). Applicant respectfully traverses this art grounds of rejection.

Initially, Applicant agrees with the Examiner regarding the failure of Alden, Citta and Barnett in disclosing or anticipating certain claim limitations present within claims 3, 6, 9 and 12. The Examiner alleges, however, that Semper discloses these particular claim limitations.

Semper is directed to a system and method providing backward compatibility of radio link protocols in a wireless network. A review of Semper indicates that Semper fails to cure the

suggestion and disclosure deficiencies of Alden in view of Citta and Barnett related to independent claims 1, 4, 7 and 10. As such, claims 3, 6, 9 and 12, dependent upon independent claims 1, 4, 7 and 10, are likewise allowable over Alden in view of Citta and Barnett and further in view of Semper at least for the reasons given above with respect to independent claims 1, 4, 7 and 10.

Applicant respectfully requests that the Examiner withdraw this art grounds of rejection. Reconsideration and issuance of the present application is respectfully requested.

35 U.S.C. §103(a) Alden in view of Citta and further in view of Kluttz

Claims 1, 4, 7, 13-28 and 33-34 are rejected under 35 U.S.C. § 103(a) as being unpatentable over Alden in view of Citta and further in viewof Kluttz. Applicant respectfully traverses this art grounds of rejection.

As will be discussed below in greater detail, even if were to assume that one of ordinary skill in the art were to have an adequate motivation or rationale to combine Alden with Citta and Kluttz, that combination would not result in Applicant's claimed invention.

Discussion of Alden

Alden is directed to a pseudo network adapter for frame capture, encapsulation and encryption. The general functionality of Alden's pseudo network adapter is discussed with respect to Figure 15, as follows:

> During operation of the elements shown in FIG. 15, the pseudo network adapter 259 registers with the network layer in the TCP/IP stack 260 that it is able to reach the IP addresses of nodes within the virtual private network 249 as shown in FIG. 14. For example, the pseudo network adapter on the client system registers that it can reach the pseudo network adapter on the server. Subsequently, a message from the tunnel client addressed to a node reachable through the virtual private network will be passed by the TCP/IP stack to the pseudo network adapter 259. The pseudo network adapter 259 then

encrypts the message, and encapsulates the message into a tunnel data frame. The pseudo network adapter 259 then passes the tunnel data frame back to the TCP/IP protocol stack 260 to be sent through to the physical network adapter in the tunnel server. The tunnel server passes the received data frame to the pseudo network adapter in the server, which de-encapsulates and decrypts the message.

(Emphasis added) (See Column 14, line 58 to Column 15, line 8 of Alden)

As will be appreciated from a review of the above-excerpt of Alden, the pseudo network adapter 259 (i) receives a message or packet, (ii) encrypts the packet, (iii) encapsulates the encrypted packet within a data frame for transmission, (iv) transmits the data frame to another pseudo network adapter where the data frame is de-encapsulated and decrypted. Accordingly, the encryption of Alden is performed at the transport layer (e.g., executing TCP/IP protocols).

Discussion of Citta

Citta is directed to a secure data packet transmission system and method. Citta teaches the transmission of a global bit packet encrypted with a global encryption key followed sequentially by individually addressed packets (i.e., intended for a subset of subscribers, and not a global broadcast) encrypted with address keys. Thus, the global packets can be data associated with a free television broadcast, and the individually addressed packets can be for a pay-per-view (PPV) television broadcast, or premium channel such as HBO, Showtime, etc.

Citta discloses a data encryption and error protection (DEEP) feature, which is a software tool that performs encryption and error correction on packets (Column 2, line 54-61 of Citta). With regard to DEEP, Citta states that "[m]emory 30 is for storing the address and address key for the particular subscriber terminal. The address and address keys are permanent and 'burned into' the memory at the factory" (Column 4, lines 60-65 of Citta). Thus, the subscriber terminals store the (i) address and (ii) address keys internally and permanently. The (i) address is used to determine what type of content is being received at the subscriber terminal (e.g., HBO,

Showtime, etc.), and the (ii) address keys are used to decrypt that content at the subscriber terminal (also, predetermined session keys are used to decrypt global packets, e.g., see column 5, lines 4-15 of Citta).

Packet decryption of global/individual packets at the subscriber terminal is discussed in detail in the following section of Citta:

> With particular reference to the flow chart [of FIG. 4], initially a counter in the subscriber terminal is reset to zero. The previously used session key is loaded into the subscriber terminal DEEP shift register, the start code is detected and the resulting CRC code (i.e. the 16 bit remainder of the processed packet) for the global packet is checked. If the CRC code matches (remainder of all zeros), it is presumed that the session key is correct and that there are no errors in the data. At that point, the counter is reset to zero and the global packet is processed for any general information therein, that is, information that is applicable to all subscriber terminals. Next the terminal address key is loaded into the DEEP shift register for processing the first received addressed data packet. Again the CRC is checked. If the CRC code is not all zeros, the packet either is addressed to a different subscriber terminal or there are errors in it. In either event, the packet is ignored. If the CRC code shows all zeros, an address comparison is made in the subscriber terminal controller to see if indeed the packet is meant for that subscriber terminal. If the address comparison shows a mismatch, the packet is ignored. If the address comparison shows a match, the packet is processed by the microprocessor and the procedure is repeated for the next two addressed packets. It is thus seen that the microprocessor only processes packets that are intended for it.
>
> *(Column 6, lines 21-47 of Citta)*

As will be appreciated from the above-excerpt of Citta, the subscriber terminal first checks whether a previously used session key (i.e., session keys are for global packets only) decrypts the global packet without errors (if errors present, packet is ignored). Next, because the global and individual packets are always sent in the same order, the subscriber terminal's address key is next used to decrypt each subsequent/sequential individual packet. If errors are present, the subscriber terminal ignores the packet; otherwise, if the CRC code indicates no errors, the subscriber terminal has sufficient authorization to decode the packet (e.g., to watch HBO, a PPV boxing match, etc.). Like Alden, Citta appears to be directed to transport-layer encryption.

Discussion of Kluttz

Kluttz, on the other hand, is directed to encrypting a stored file or document. Referring to Figures 3 and 4 of Kluttz, Kluttz teaches partitioning a document into multiple portions, and applying a different level of encryption to each portion. Portions associated with "higher" level encryption are encrypted with a higher-level specific encryption key, as well as any "lower" level encryption keys. Thus, more confidential material is protected by both the higher level encryption key as well as all lower level encryption keys. As will be appreciated by one of ordinary skill in the art, the encryption of Kluttz is directed to a file storage protocol executed at the application layer, and not at a transport layer (as in Alden and Citta).

Combination of Alden, Citta and Kluttz Could Not Result in Claimed Invention

Even assuming for the sake of argument that one of ordinary skill in the art could find some motivation to combine Alden, Citta and Kluttz, that combination would not result in the claimed invention. The methodologies associated with encryption of file storage documents, such as MS Word documents, MS Excel documents, etc., cannot simply be imported into the transport layer for encrypting TCP/IP packets. As will now be described in detail, there are fundamental differences between encryption performed at the file storage layer, or "application layer", and encryption performed at the TCP/IP layer, or "transport layer".

In Alden, the pseudo network adapter 259 is essentially "dumb". In other words, the pseudo network adapter 259 does not have any special knowledge regarding any particular packet that is encrypted/encapsulated, but rather simply encrypts/encapsulates any received packets. As is known in the art, in preparing a file document for transmission at the transport layer, the file document is broken up into a plurality of packets, such as TCP/IP packets, for transmission. The

pseudo network adapter 259 does not evaluate the "content" of any packets, nor does the pseudo network adapter 259 evaluate or even consider the "document" from which individual packets were generated. Such actions simply are not performed at the transport layer.

Likewise, in Citta, the address of a transport-layer packet is used to determine what type of content is being received at the subscriber terminal (e.g., HBO, Showtime, etc.), and the address keys are used to decrypt that content at the subscriber terminal. The subscriber is not aware of what the content is that is being sent, but simply attempts to decode based on its personal address key, which is associated with the subscriber's permissions. If the packet cannot be decoded it is simply discarded.

Accordingly, Kluttz's method of partitioning a storage file document into different portions associated with different levels of encryptions makes no sense at the transport layer, nor is there any comparable transport layer operation that could be achieved based on the teachings of Alden and/or what is known in the art. In other words, how could a document be partitioned when the pseudo network adapter 259 of Alden, or the subscriber in Citta, only has knowledge of an individual packet with no knowledge of that packet's association with any particular document? How could the pseudo network adapter 259 in Alden, or the subscriber in Citta, associate that packet with a corresponding portion of a document that is associated with a given level of security/encryption? Many more questions could be raised regarding this alleged "obvious" implementation or combination.

Instead of combining the references in the manner alleged by the Examiner, Applicant respectfully submits that a much more likely combination of Alden, Citta and Kluttz would simply be to (i) encrypt a file storage document at the application layer as indicated by Figure 2 of Kluttz and (ii) if it is determined to send the file storage document to another entity, to break up the file storage document into individual packets as is known in the art and process the

individual packets through the pseudo network adapter 259 as described by Alden. At the receiving end, a subscriber would receive the packet, as in Citta, and attempt to decode/decrypt the packet based on its address key. In other words, because Alden or Citta and Kluttz deal with encryption at different layers, their processes would be applied separately, and not meshed together in the manner suggested suggested by the Examiner. Applicant notes that the claims would not read upon Kluttz, Citta and Alden combined in this manner.

In view of the above remarks, Applicant respectfully submits that the combination of Alden, Citta and Kluttz cannot result in Applicant's claimed invention. In particular, the combination of Alden, Citta and Kluttz cannot disclose or suggest "encrypting a first data frame based on a first unique code in a first communication device, said first unique code being derived from a first sequential code ... encrypting a second data frame based on a second unique code in the first communication device, said second unique code being derived from a second sequential code ... wherein said first portion of said first sequential code and said first portion of said second sequential code identify the same relative portions of said first and second sequential codes, and said second portion of said second sequential code represents a successive relative portion with respect to said second portion of said first sequential code" as recited in independent claim 1 and similarly recited in independent claims 4, 7, 10, 13, 17, 21 and 25, 33-34.

Further, Applicant has discussed above how Alden, Citta and Barnett fail to disclose or suggest deriving an encryption key that is used to encrypt a packet from a given code and then including the given code in the encrypted packet. A review of Kluttz, which is not even directed to packet-layer encryption at the transport layer, indicates that Kluttz is similarly deficient. Accordingly, Applicant respectfully submits that the combination of Alden, Citta and Kluttz fails to disclose or suggest "encrypting a first data frame based on a first unique code ... said first

unique code being *derived from a first sequential code*" and "encapsulating said first encrypted data frame in a first transport frame, *said first transport frame comprising a first portion and a second portion of said first sequential code*" (Emphasis added) as recited in independent claim 1 and similarly recited in independent claims 4, 7, 10, 13, 17, 21 and 25.

As such, claims 14-16, 18-20, 20-24, 26-28 and 33-34, dependent upon independent claims 1, 13, 17, 21 and 25, respectively, are likewise allowable over the combination of Alden, Citta and Kluttz at least for the reasons given above with respect to independent claims 1, 13, 17, 21 and 25, respectively.

Applicant respectfully requests that the Examiner withdraw this art grounds of rejection.

35 U.S.C. 103(a) Alden in view of Citta and further in view of Kluttz and Perlman

Claims 2, 5, 8 and 11 stand rejected under 35 USC § 103(a) as being unpatentable over Alden in view of Citta and further in view of Kluttz and Perlman (US 6363480). Applicant respectfully traverses this art grounds of rejection.

Initially, Applicant agrees with the Examiner regarding the failure of Alden, Citta and Kluttz in disclosing or anticipating certain claim limitations present within claims 2, 5, 8 and 11. The Examiner alleges, however, that Perlman discloses these particular claim limitations.

Perlman is directed to a method of ephemeral decryptability. A review of Perlman indicates that Perlman fails to cure the suggestion and disclosure deficiencies of Alden in view of Citta and Kluttz related to independent claims 1, 4, 7 and 10. As such, claims 2, 5, 8 and 11, dependent upon independent claims 1, 4, 7 and 10, are likewise allowable over Alden in view of Citta and Kluttz and further in view of Perlman at least for the reasons given above with respect to independent claims 1, 4, 7 and 10.

Applicant respectfully requests that the Examiner withdraw this art grounds of rejection.

35 U.S.C. 103(a) Alden in view of Citta and Kluttz and further in view of Semper

Claims 3, 6, 9 and 12 stand rejected under 35 USC § 103(a) as being unpatentable over Aldre in view of Citta and Kluttz and further in view of Semper. Applicant respectfully traverses this art grounds of rejection.

Initially, Applicant agrees with the Examiner regarding the failure of Alden, Citta and Kluttz in disclosing or anticipating certain claim limitations present within claims 3, 6, 9 and 12. The Examiner alleges, however, that Semper discloses these particular claim limitations.

Semper is directed to a system and method providing backward compatibility of radio link protocols in a wireless network. A review of Semper indicates that Semper fails to cure the suggestion and disclosure deficiencies of Alden in view of Citta and Kluttz related to independent claims 1, 4, 7 and 10. As such, claims 3, 6, 9 and 12, dependent upon independent claims 1, 4, 7 and 10, are likewise allowable over Alden in view of Citta and Kluttz and further in view of Semper at least for the reasons given above with respect to independent claims 1, 4, 7 and 10.

Applicant respectfully requests that the Examiner withdraw this art grounds of rejection.

Reconsideration and issuance of the present application is respectfully requested.

Conclusion

In light of the amendments contained herein, Applicants submit that the application is in condition for allowance, for which early action is requested.

Please charge any fees or overpayments that may be due with this response to Deposit Account No. 17-0026.

Respectfully submitted,

Dated: September 25, 2008

By: _____
Raphael Freiwirth
Reg. No. 52,918
(858) 651-0777

QUALCOMM Incorporated
Attn: Patent Department
5775 Morehouse Drive
San Diego, California 92121-1714
Telephone: (858) 658-5787
Facsimile: (858) 658-2502